UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/923,075	08/06/2001	Lynn Henry Wheeler	10399-34383	1892

26702 7590 09/11/2007

MORRIS, MANNING & MARTIN LLP
1600 ATLANTA FINANCIAL CENTER
3343 PEACHTREE ROAD NE
ATLANTA, GA 30326

EXAMINER	
PYZOCHA, MICHAEL J	
ART UNIT	**PAPER NUMBER**
2137	

MAIL DATE	DELIVERY MODE
09/11/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/923,075	WHEELER ET AL.	
	Examiner	Art Unit	
	Michael Pyzocha	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 January 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-29* is/are pending in the application.

4a) Of the above claim(s) *1-11* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *12-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-29 are pending. Claims 1-11 have been withdrawn from consideration.

2. Amendment filed 01/02/2007 has been received and considered.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless -
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 12, 15-17, 21, and 24-26 are rejected under 35 U.S.C. 102(b) as being anticipated by Fischer (US 5422953).

As per claims 12 and 21, Fischer discloses a method and system for generating a digital signature for use as a random number for utilization in an application requiring the random number, the method comprising the steps of: storing a private key of a public/private key pair within a device (see figure 1 numeral 6 and column 3 lines 44-46 and column 7 lines 56-59); generating within the device a digital signature using the private key and a digital signature algorithm (see column 7

lines 56-62); providing to the application external to the device the generated digital signature as the random number for use by the application (see 7 lines 63-67).

As per claims 15 and 24, Fischer discloses the digital signature is generated within a computer chip within the device (see figure 1 and column 3 lines 25-38).

As per claims 16 and 25, Fischer discloses the computer chip itself includes a random number generator (see figure 1 numeral 10 and column 4 lines 1-15).

As per claims 17 and 26, Fischer discloses the digital signature is generated within the computer ship using the private key and a random number obtained from the random number generator (see column 4 lines 1-15).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 13 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fischer as applied to claims 12 and 21 above, in view of Binding et al. (US 6775772).

As per claims 13 and 22, Fischer fails to disclose the use of the digital signature as a safeguard against a replay attack.

However, Binding et al. teaches the use of a digital signature on a nonce as a safeguard against a replay attack (see column 9 line 64 through column 10 line 11).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the digital signature as a safeguard against a replay attack.

Motivation to do so would have been to verify the identity of each party in the communication.

7. Claims 14 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fischer as applied to claims 12 and 21 above, in view of Ellison (US 6073237).

As per claims 14 and 23, Fischer fails to disclose generating a session key based on the digital signature.

However, Ellison teaches such generation of a session key based on a digital signature (see column 4 lines 62-67).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to generate a session key based on the digital signature of Fischer.

Motivation to do so would have been that using a digital signature increases the security in the system because the session key can only be generated after the verification function authenticates a digital signature.

8. Claims 18 and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fischer as applied to claims 17 and 26 above, and further in view of Applicant's Admitted Prior Art (hereinafter AAPA).

As per claims 18 and 27, Fischer discloses the use of other digital signature algorithms (see column 3 lines 56-60) but fails to explicitly disclose the use of an elliptical curve digital signature algorithm.

However, AAPA teaches that an elliptical curve digital signature algorithm is a common way to generate a digital signature (see paragraph 146 [page 26 line 32-36]).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use an elliptical curve digital signature algorithm because doing so is a common way of generating a digital signature.

9. Claims 19, 20, 28, and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fischer in view of AAPA as applied to claim 18 and 27 above, and further in view of Wang (US 6594759).

As per claims 19, 20, 28 and 29, Fischer in view of AAPA discloses the chip being tamper resistant (see Fischer column 3 lines 31-38), but fails to explicitly disclose the random number generator is inaccessible from outside the computer chip.

However, Wang teaches that the random number generator can be used solely by a computer chip (see column 13 line 49 through column 14 line 6).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to make the random number generator of the modified Fischer and AAPA system be inaccessible from the outside.

Motivation to do so would have been to increase the security of the system.

Response to Arguments

10. Applicant's arguments with respect to claims 12-29 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

11. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS**

ACTION IS MADE FINAL. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

12. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Giniger et al. teaches a method of generating digital signatures.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Pyzocha whose telephone number is (571) 272-3875. The examiner can normally be reached on 7:00am - 4:30pm first Fridays of the bi-week off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MJP

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER